

Privacy Policy

Policy Owner:	General Manager - Finance & Governance
Department and Unit:	Finance & Governance – Governance
Document UIN:	1PS8
Effective Date:	January 2024
Review Date:	January 2027

Approval

Approved by	Signature	Date
Board	Board Meeting 250 6 th December 2023	January 2024

Table of Contents

Policy.....	2
Definitions	2
Collection of Personal Information	3
Use of Personal Information	7
Disclosure of Personal Information	8
Access and correction of Personal Information.....	10
Protection of Information	11
Variations.....	13
Privacy Contact Officer.....	13
Complaints and Feedback	14
Risk and Quality Approach	14
Related Organisational Documents	14

Policy

Cancer Council SA (**CCSA**) is committed to ensuring a responsible, transparent and ethical framework is applied in accordance with this Privacy Policy (**Policy**) and Commonwealth legislative requirements. CCSA is bound by the Australian Privacy Principles (**APPs**) and the *Privacy Act 1988* (Cth) (**Privacy Act**). This Policy regulates the ways in which CCSA collects, holds, maintains, uses and discloses personal information, including health information.

This Policy applies when individuals:

- use any of CCSA's products and services;
- visit CCSA's main website at **cancersa.org.au** or any of our affiliated websites (**Sites**), visit any of our social media channels or subscribe to our mailing lists (**Channels**);
- are employed by us or are seeking employment with us;
- are one of CCSA's employees, board members, volunteers, donors or contractors; or
- persons who are otherwise engaged with CCSA in its activities and operations.

By providing us with personal information, individuals consent to their personal information being collected, held, used and disclosed in accordance with this Policy. This Policy is in addition to any other applicable terms and conditions that may apply to individuals relationship and/or engagement with us. By continuing to use our products, services, Sites or Channels, or otherwise continuing to deal with us, users accept any changes made from time to time and this Policy as it applies. However, if an individual does not agree to an amendment, they must discontinue their interactions or dealings with us (e.g. by not using our Sites, products or services or by unsubscribing from our Channels).

Definitions

Personal Information – is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and includes information such as:

- name, date of birth, gender and contact information
- health information
- credit/debit card information

-
- employee record information
 - tax file number information

Sensitive Information – is personal information that may include information or an opinion about an individual’s:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- sexual orientation or practices
- health or genetic information
- some aspects of biometric information.

Notifiable Data Breach – is when a data breach occurs and the following criteria is met:

- There is unauthorised access to, or disclosure of personal information held by CCSA (or information is lost in circumstances where unauthorised access or disclosure is likely to occur) and
- This is likely to result in serious harm to any of the individuals to whom the information relates and
- CCSA has been unable to prevent the likely risk of serious harm with remedial action.

If this criterion is met, the Office of the Australian Information Commissioner must be notified of the data breach.

Privacy Impact Assessment (PIA) – is a systematic assessment of a new initiative / project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them.

Serious Privacy Incident: A privacy breach which may result in a Notifiable Data Breach, reputational or financial damage to CCSA.

Collection of Personal Information

Whose Information CCSA Collects

CCSA collects information only where it is necessary to enable the organisation to meet its business functions. Information may be collected from people who are connected to its operations and activities including:

- current and former employees, board members, volunteers;
-

-
- donors, research study participants, recipients of support services;
 - participants in advocacy campaigns or health promotion projects;
 - next-of-kin or emergency contacts;
 - health professionals; and
 - suppliers, contractors, and service providers.

Personal information CCSA may collect includes (as applicable):

For Customers:

- contact information such as full name (first and last), e-mail address, current postal address and phone numbers;
- identifying and diversity information (including date of birth, gender, and whether information regarding Aboriginal and/or Torres Strait Islander descent);
- information provided to us where individuals share their cancer experience story (including details of the experience, such as cancer diagnosis and treatment);
- health and medical information (e.g. medical history, contact details for medical practitioners and treatment providers etc.) as needed to determine eligibility for our counselling, accommodation, social work or research services and program, and to provide those services and programs;
- insurance policies and details;
- opinions via surveys and questionnaires;
- records of our communications or dealings with individuals, including any complaints, incidents, requests or queries;
- details relating to the goods and services a person has enquired about or have obtained from CCSA, including any additional information necessary to deliver those goods and services and respond to enquiries;
- details relating to donations to CCSA;
- any relevant financial information (including bank account details, credit card details, billing address and invoice details);
- personal identification documents (e.g. to administer refunds, to enable access to information);
- username and password when setting up an account on our website; and

-
- any other personal information that may be required to facilitate an individual's dealings with us and/or to assist us in conducting our business, providing and marketing our services and meeting our legal obligations.

For Job Applicants, Employees, Volunteers or Contractors:

- work and/or personal contact details (e.g. telephone, email, address etc);
- financial information (e.g. bank account details or payment history for invoicing and/or payroll purposes);
- superannuation fund details;
- government identifiers (e.g. tax file number, driver's licence, passport and/or visa details);
- diversity information, which might include gender, ethnicity, languages spoken, relationship status etc;
- relevant health information
- personal information from personal, professional or trade references; and
- information about occupation, employment history, education and suitability for the role or relationship, including criminal history, social media profiles and whether the individual holds any police or working with children clearances required for the role.

Where possible, CCSA will sight government identifier documents and record 'as sighted' without retaining a copy. If it is necessary to take copies of government identifier documents, they will be destroyed upon the completion of the identity check.

Where possible and if requested, CCSA enables customers to interact with them anonymously or using a pseudonym (such as when using Cancer Council SA's 13 11 20). Anonymity or pseudonymity however, may affect the capacity of CCSA to provide some services. This is communicated on a case-by-case basis.

How CCSA Collects Information

CCSA may collect personal information from individuals in different ways. CCSA will generally collect personal information directly, including when a person:

-
- purchases a product or use a service (e.g. social work, counselling, nursing advice), provided by CCSA;
 - provides a donation or bequest of funds;
 - interacts with us (e.g. by email or phone) or submits information to our Sites or Channels;
 - provides information or opinions via surveys or questionnaires;
 - utilises accommodation services at CCSA;
 - attends or organise a CCSA event;
 - provides feedback to us or completes a survey; and
 - participates in CCSA research.

CCSA may also obtain personal information from third parties such as contractors, including fundraising/marketing service providers, health professionals and social and community workers.

If information has been provided to CCSA about another person, the individual warrants that they have that person's permission to do so. Obligations under the Privacy Act may also mean that they need to tell that person about the disclosure and let them know that they have a right to access their personal information and that we will handle their personal information in accordance with this Policy.

Website Cookies

To improve our Sites and advertising and to help us better understand browsing behaviour, when individuals use our Sites we may use website measurement software and other analytics tools and services (including Google Analytics) to gather information such as traffic patterns, mouse click activity, IP addresses, and any other information that individuals provide through use of our Sites. We may also use analytics tools available on our Channels. This information is aggregated and anonymised so that a person cannot be identified.

This information is gathered as part of CCSA's business activities and to assist us with any operational difficulties, gain efficiencies, understand browsing behaviour or provide support with our web-based services.

Like many other websites on the internet, CCSA may use 'cookies' to store and track information about individuals when they are on our Sites or Channels. A cookie is a data file that is sent to a browser from

a web server and stored on the users computer (or other device), then sent back to the server by the browser each time they access certain sections of our Sites or Channels.

This information helps us to remember preferences and can help us to provide a tailored experience and customised content and material on our Sites and Channels. This information may be retained in an anonymous or aggregated form after we have erased personal information that identifies users from our systems.

Users can choose to disable cookies via the device's website browser settings. However, if they choose to reject cookies, they may not be able to use or access some features of the services that we offer.

CCSA provides links or references to other websites from our Sites or Channels. This Policy does not apply to those websites and we take no responsibility for any information collected by such third parties.

Use of Personal Information

CCSA collects personal information for the primary purpose to carry out its functions and activities, including to provide support to South Australians impacted by cancer, undertake research and support the reduction in preventable cancers through advocacy.

To support these functions, the purposes which CCSA may use and disclose personal information includes:

- the provision of our services, including but not limited to counselling, support services, and accommodation;
- undertake fundraising, including the processing of donations and/or grants;
- the processing of scholarships and/or awards;
- undertaking and publishing results of research and related documentation;
- processing and communicating information about orders;
- supporting the work of contractors, employees, and volunteers within CCSA;
- providing direct marketing (including joint marketing) about our products, services, events, fundraising and other promotional activities, either in relation to us, other Cancer Councils, or other similar charities and causes;
- to respond to any feedback, queries or complaints;

-
- the improvement of services (including contacting individuals regarding participation in surveys);
 - to maintain and administer employee and contractor records and payments;
 - to assess suitability of potential employees or contractors and performance of current employees or contractors;
 - to ensure health and safety on our premises;
 - if required, the verification of identity in communicating with individuals;
 - to comply with our legal obligations and reporting obligations; and
 - as otherwise required for the conduct of our business.

Opting Out of Direct Marketing Communications

CCSA may use personal information collected for related secondary purposes to provide cancer support, research and prevention activities. This includes sending general and promotional material by post, email, telephone or SMS or face to face to identify programs or services an individual may be interested in, and other promotions, events and offers. CCSA will provide individuals with information regarding the secondary purposes at time of collection and provides the opportunity for individuals to withdraw consent by utilising the opt-out link on all marketing communications or by contacting the Privacy Officer directly.

Disclosure of Personal Information

Disclose to Third Parties

CCSA may disclose personal information for the purpose for which it was collected (or a related secondary purpose) and otherwise where permitted or required by law or with the individual's consent.

Some of the recipients we may disclose personal information to may include:

- External support services – to health care professionals, lawyers, counsellors, volunteers and other external support service providers;
 - Third party researchers – to support research studies in relation to cancer, as well as diagnosis, treatment and cures
-

(provided that informed consent has been obtained and in accordance with research ethics and requirements);

- Third-party service providers, government departments and agencies, and medical health personnel that may assist CCSA with financial support, transportation, accommodation services, counselling, fundraising, support services;
- CCSA's contractors, service providers and agents, who perform services on CCSA's behalf, such as professional advisory, marketing and advertising, data analysis, recruitment, website and information technology services (including offshore cloud computing service providers), business and administrative services, database contractors and telemarketing agencies; and
- Cancer Council Australia and State and Territory Cancer Councils that are members of Cancer Council Australia.

Where we do disclose personal information, we ensure that only the minimum data required is disclosed, it is deidentified where appropriate and we make investigations into the data security policies and procedures of the recipients to protect the data where possible.

Cross Border Disclosures

CCSA may from time to time engage an overseas recipient to provide services to us, such as cloud-based storage solutions. As a result, personal information provided to CCSA may be disclosed to, and stored at, destinations outside Australia. Please click [here](#) to review the list of current countries outside Australia which constitute a cross border disclosure.

Please note that the use of overseas service providers to store personal information will not always involve a disclosure of personal information. However, by providing us with personal information, individuals consent to the storage of such information on overseas servers and acknowledge that Australian Privacy Principle (APP) 8.1 will not apply to such disclosure. For the avoidance of doubt, in the event that an overseas recipient breaches the APPs, that entity will not be bound by, and the individual will not be able seek redress under, the Privacy Act.

**Access and
correction of
Personal
Information**

Access

Individuals are entitled to access the personal information we hold about them and may do so by contacting our Privacy Officer. In processing the request, we will comply with our obligations under the Privacy Act, noting that we may need to verify an individual's identity before we allow them to access their personal information, and are permitted to withhold the disclosure of personal information in prescribed circumstances.

Requests for information and or alteration can be made directly to the Privacy Officer in writing (see details below). The requester must identify, as clearly as possible, their full name, the type(s) of information they require, or outline their requested changes.

CCSA will respond to the request to provide access to / change personal information within 30 days.

CCSA is not required, under law, to grant access in certain circumstances such as where:

- access would pose a serious threat to the life, safety or health of any individual or to public health or public safety
- access would have an unreasonable impact on the privacy of other individuals
- the request is frivolous or vexatious
- denying access is required or authorised by a law or a court or tribunal order
- access would be unlawful, or
- access may prejudice commercial negotiations, legal proceedings, enforcement activities or appropriate action being taken in respect of a suspected unlawful activity or serious misconduct.

If CCSA refuses to grant access to personal information, CCSA will provide the individual with the rationale for this decision in writing and the avenues for complaining about CCSA's response, unless it is unreasonable to do so.

CCSA may charge a reasonable fee for facilitating an access request (being limited to the amount of the reasonable expenses incurred in

responding to the request, for example photocopying and administrative expenses).

Correction

In the event an individual believes the personal information CCSA holds about them is inaccurate, incomplete or out of date, they are required to contact our Privacy Officer. If they satisfy CCSA that any personal information we hold about them is not accurate, complete or up-to-date, we will amend our records accordingly.

CCSA will respond to the request to provide access to / change personal information within 30 days.

Protection of Information

Data Security

CCSA takes all reasonable steps to protect the personal information it holds from misuse, interference, loss, and from unauthorised access, modification, or disclosure.

To uphold strong protocols of information protection, CCSA maintains strict protocols regarding the storage, transfer and destruction of the information it holds, including:

- monitoring of external and internal cyber security threats
- software security and stringent password policies;
- network firewalls;
- CCTV video surveillance in key public spaces within CCSA premises
- physical security measures; and
- keeping access to information limited by role and requirement within CCSA.

Hard copy information is generally stored at the CCSA office, which is secured to prevent entry by unauthorised people. Any hard copy personal information not actively being used is archived with a third-party provider of secure archiving services.

Individual's personal information may only be stored on a CCSA protected electronic device, on a CCSA database, including cloud storage or other approved third-party database storage. All personal and sensitive information must be authorised by the General Manager for release in relation to their individual departments. Oversight of the electronic storage of information is the

responsibility of the CCSA Digital department, including oversight of any offshore transfer of data. New software implemented within CCSA must be approved by the Digital Team and a Privacy Impact Assessment may be undertaken.

CCSA must ensure that access to personal information held by CCSA, including client's personal information, is only permitted on a need-to-know basis and by individuals (employees, volunteers, external parties) with express authority to access the information for a specified purpose.

Investigations are undertaken for new and existing external parties with whom we share data to ensure that appropriate security practices are maintained by external parties in relation to the data that CCSA is sharing.

Data Retention and Destruction

CCSA maintains a Data Retention & Disposal Schedule in accordance with legislative minimum requirements of data retention. Personal and sensitive information is stored for only as long as it is required for the purpose for which it was collected, unless a longer retention period is required for the purpose of discharging our legal, accounting and reporting requirements.

Where CCSA no longer requires an individual's personal information, we will use reasonable endeavours to comply with our legal obligations in respect of that information (e.g. by de-identifying or destroying such personal information).

Privacy Breach

A privacy breach is when information is inadvertently disclosed to an unintended or non-consented party through human error or maliciously. This may also be referred to as a data breach when this involves electronic information. All privacy breaches at CCSA must be communicated to the Privacy Officer and if relevant, to the General Manager - Digital and must be handled in accordance with the CCSA Data Breach Procedure. In the event of a notifiable breach, CCSA will proactively communicate with the impacted individuals about how the incident will be managed and how they will be supported during an incident resolution process.

All privacy related incidents must be documented within the CCSA incident management system and serious incidents must be escalated to Chief Executive. The Chief Executive will determine whether the incident is escalated to the Board. Serious incidents which are notifiable data breaches are dealt with as per the Notifiable Data Breach section below.

Notifiable Data Breach

In the event of a serious data breach, CCSA is required to comply with the Notifiable Data Breach Scheme (NDBS) requirements including contacting the Office of the Australian Information Commissioner. Notifiable Data Breaches and remedial actions are reported to the Board by the Chief Executive.

Variations

The Policy is current at January 2024. The Policy is reviewed a minimum of every 3 years or as required from time to time to reflect changes in the law and technology, changes in CCSA's business functions, operations or practices, or in response to an opportunity for improvement or change in business environment.

Our Privacy Policy Statement is available on the CCSA website and all changes to the Policy will be published on the website.

Privacy Officer

CCSA maintains an appointed Privacy Officer who is responsible for advising on matters relating to privacy and is the contact person for all enquires in relation to privacy matters. They can be contacted on:

Privacy Officer:

Call: (08) 8291 4111

Facsimile: (08) 8291 4122

Email: privacy@cancersa.org.au

Write to us: PO Box 929

Unley BC SA 5061

The Privacy Officer is responsible for the oversight of the Privacy Policy and provides broader consultation in relation to ensuring all employees are familiar with their requirements to maintain privacy.

Furthermore, It is the responsibility of the People, Safety and Culture team in consultation with the Privacy Officer to ensure all team members are provided sufficient training regarding their responsibilities to maintain privacy at induction and ongoing. Privacy

	<p>expectations are also communicated through individual position descriptions and confidentiality agreements utilised across CCSA's business operations.</p>
--	---

<p>Complaints and Feedback</p>	<p>If an individual has any queries or complaints relating to the manner in which their personal information was handled, or in relation to the Policy, they can contact the Privacy Officer directly.</p> <p>CCSA endeavours to respond to complaints and queries within 30 days of the date of receipt. If an individual is dissatisfied with CCSA's response or handling of their complaint, they can contact the Office of the Australian Information Commissioner at: GPO Box 5218, Sydney NSW 2001 or by email to enquiries@oaic.gov.au.</p>
---------------------------------------	---

<p>Risk and Quality Approach</p>	<p>CCSA reviews risk associated with information security and privacy practices routinely in accordance with the Risk Management Framework and is committed to continuous quality improvement. Opportunities for improvement in relation to information security and privacy may come from audit activity, incident response, changes in technology and feedback from individuals.</p>
---	--

<p>Related Organisational Documents</p>	<ul style="list-style-type: none"> • Compliance Policy • Code of Conduct Policy • Feedback and Complaints Policy • Retention & Disposal Schedule • Data Breach Procedure • Privacy Policy Statement (Public Facing)
--	---

<p>References</p>	<ul style="list-style-type: none"> • Office of the Australian Information Commissioner (OAIC) • Privacy Act 1988 (Cth) • Charities Act 2013 (Cth) • Surveillance Devices Act 2016 (SA) • Australian Privacy Principles
--------------------------	---
